Unsere City wird smart!
OURS. Not MINES
WIKI
UN
EU
IETF
TLS
WIKI
Schluss mit WIRSING. Digitale Verwaltung JETZT!
Mein Gesicht gehört mir.
Our world is not for sale!
Abwärme für Wärmenetz statt Flusserwärmung
Nachhaltige Software
Fehler in Zeile 42
Macrosoft
Software ist wie ein Gesetz!
Ich will mein GESETZ
Free and Open your Software NOW!
Unterstützt keine Monopole!
Hackerthon
WIKI
Free and Open Source
Ziel: FOSS Cloud Computing
Freie Software?
1. Quellcode lesen
2. Quellcode ändern
3. Quellcode weitergeben
IT-Produkte Second Hand Umsonst & Reparatur
Lehrer und IT
KLIMA FORSCHUNGSINSTITUT
BILDUNGSCHANCEN
Spielend Zukunft gestalten
Umwelt-Campus Birkenfeld

Ein Unternehmen der **EWN** Gruppe

EWN
Entsorgungswerk für
Nuklearanlagen

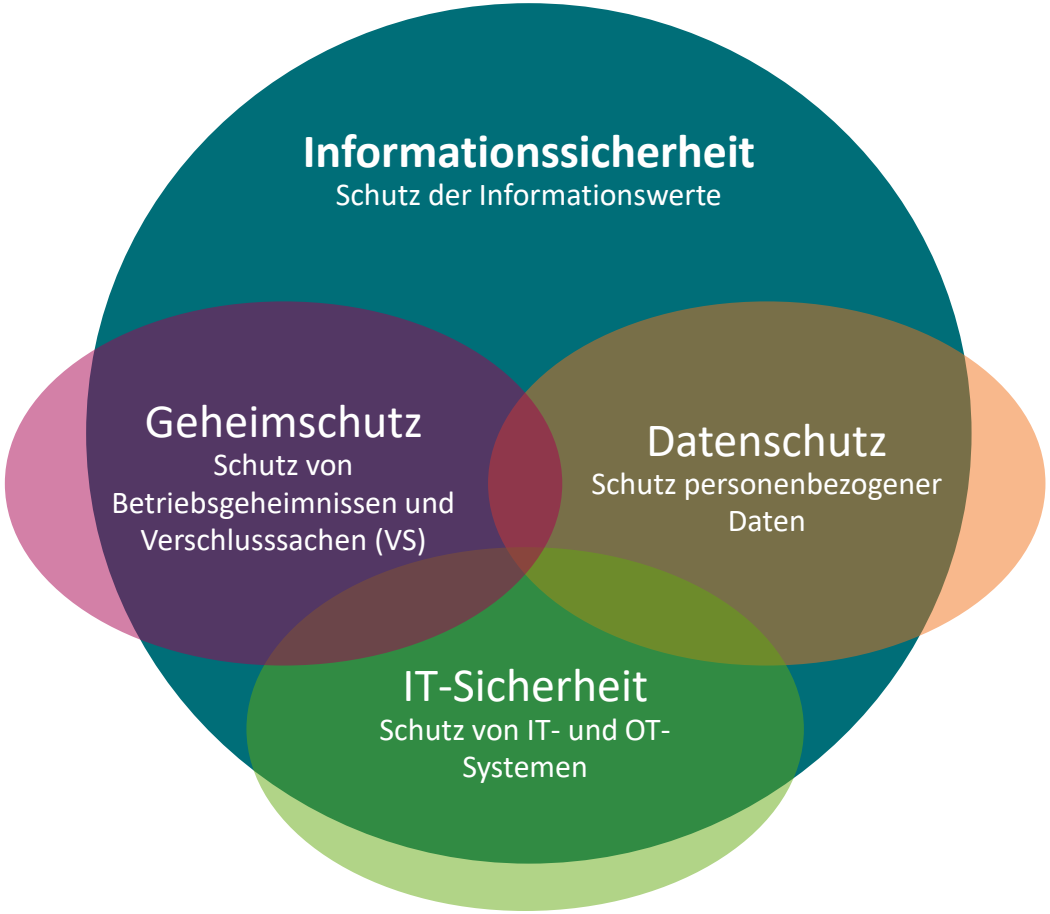
INFORMATIONSSICHERHEIT

IT-Sicherheit - Geheimhaltung - Datenschutz

Angela Bialke
Datenschutzbeauftragte

Stand: 06.01.2026

Worum geht es heute?



INFORMATIONSSICHERHEIT

Sicherheit und Schutz betrieblicher Daten

Was sind Informationen?

- Jeglichen Wissen über Objekte, Personen oder Sachverhalt ist Information
- Dabei können Informationen auf Papier, in IT-Systemen oder auch in den Köpfen der Benutzer „gespeichert“ sein.
- Darstellungsformen
  - Schriftstücke
  - Zeichnungen
  - Karten
  - Fotokopien/Lichtbildmaterial
  - Elektronische Datenträger
  - Gesprochenes Wort etc.

Was ist Informationssicherheit?

- Die Sicherheit von Informationen wird bedroht durch:
  - vorsätzliche Handlungen: Diebstahl, Erpressung
  - höhere Gewalt: Feuer, Wasser, Sturm, Erdbeben
  - Technische Fehler: nach einem missglückten Software-Update funktionieren Anwendungen nicht mehr oder Daten werden unbemerkt verändert.
  - Menschliche Fehler: vertrauliche Informationen werden versehentlich von einem Mitarbeiter an Unbefugte weitergegeben.
  - Fehlplanung: ein wichtiger Geschäftsprozess verzögert sich, weil die einzige Mitarbeiterin, die mit der Anwendungssoftware vertraut ist, erkrankt ist.

Informationssicherheit hat das Ziel, Informationen unabhängig von Art und Herkunft zu schützen.

Zuständigkeit

- Bei Fragen oder Ereignissen, welche die Informationssicherheit betreffen könnten, wenden Sie sich bitte an die für die Standorte Lubmin/Rubenow und Rheinsberg/Menz zuständigen
  Informationssicherheitsbeauftragten der EWN (ISB):

Hendrik Gralla
Telefon +49 38354 4-9313

it-sicherheit@ewn-gmbh.de

Stellvertreter:
Alexander Förster
Telefon +49 38354 4-5824

GEHEIMSCHUTZ

Verschlusssachen (VS) - Betriebsgeheimnisse

Geheimschutz: Ziel und Anlass

- Kerntechnische Anlagen der ehemaligen Kernkraftwerke Greifswald (KGR) und Rheinsberg (KKR) sowie das Zwischenlager Nord (ZLN) sind besonders zu schützende Objekte. Darum:
  - Sind wirksame Maßnahmen zum Schutz erforderlich.
  - Dürfen viele der Maßnahmen potentiellen Angreifern nicht bekannt werden, weshalb
    - über den Inhalt Verschwiegenheit zu wahren ist und
    - diese Informationen dazu unter Verschluss zu halten sind.
  - Die Geheimhaltung ist aufgrund öffentlich-rechtlicher Vorschriften verpflichtend:
    - Verschlusssachenanweisung M-V[1)]
    - Geheimschutzhandbuch[2)]

1) Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA) Mecklenburg-Vorpommern
2) GHB; steht öffentlich im Internet zur Verfügung

Verschlusssachen (VS)

- VS sind im **öffentlichen Interesse** geheimhaltungswürdige Tatsachen, Gegenstände, Erkenntnisse.
- VS werden von amtlicher Stelle eingestuft und durch einen schriftlichen VS-Auftrag übergeben.
- Eine Verschlusssache kann sein:
  - STRENG GEHEIM
  - GEHEIM
  - VS-VERTRAULICH oder
  - VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)
- Die EWN kann aufgrund ihres Auftrages die Kennzeichnung VS-NfD eigenverantwortlich benutzen.

Umgang mit Verschlusssachen

- Von einer Verschlusssache dürfen nur Personen Kenntnis erhalten, die auf Grund ihrer Aufgabenerfüllung Kenntnis haben müssen.[1)]

Grundsatz: „Kenntnis nur, wenn nötig“

- Durch die (Haupt-)Abteilungsleitung ist für Mitarbeitende, die Aufgrund ihres Einsatzbereiches von Verschlusssachen Kenntnis erlangen müssen/können, jährlich eine Unterweisung zu veranlassen gemäß der Richtlinie:

„Behandlung von Verschlusssachen“[2)]

- Diese Richtlinie gilt für Mitarbeitende der EWN GmbH sowie für Auftragnehmer und deren Mitarbeitende die Behandlung von Verschlusssachen.

1) Sicherheitsüberprüfungsgesetz – SÜG §4 Abs. 1a)
2) Konventionelles Regelwerk F1.2 RL 01 „Umgang mit Verschlusssachen“

Zuverlässigkeitsüberprüfung und Sicherheitsüberprüfung

Zuverlässigkeitsüberprüfung

- Überprüfung **aller Beschäftigten** der EWN nach Maßgabe des § 12b des Atomgesetzes in Verbindung mit der Atomrechtlichen Zuverlässigkeitsüberprüfungs-Verordnung (AtZüV)

Sicherheitsüberprüfung

- Überprüfung von Personen, die
  - sicherheitsempfindlichen Tätigkeiten ausüben (sollen) oder
  - mit Verschlusssachen umgehen müssen/können, die als VS-VERTRAULICH oder höher eingestuft sind.
- Grundlage: Sicherheitsüberprüfungsgesetz M-V (SÜG M-V)

Betriebsgeheimnisse

Betriebsgeheimnisse:

- sind im **betrieblichen Interesse** schutzbedürftige Informationen
- müssen durch besondere Maßnahmen entsprechend ihrer Schutzbedürftigkeit von Unbefugten ferngehalten werden

- Betriebsgeheimnisse können sein
  - was im eigenem Unternehmen erarbeitet wurden
  - was für den Fortbestand/Aufgabenstellung des Unternehmens wichtig sind
  - was einen Fortschritt gegenüber dem allgem. Stand der Technik darstellt
  - was die eigene Überlegenheit gegenüber der Konkurrenz begründet bzw. Wettbewerbsvorteile verschaffen kann
  - was nicht verloren gehen soll
  - was ggf. gewinnbringend anderswo eingesetzt werden kann

Umgang mit Betriebsgeheimnissen

- Handhabung von Betriebsgeheimnissen (Aufbewahrung, Vernichtung, Weitergabe/Versand und Kommunikation) erfolgt analog zur Handhabung von VS-NfD:

„Kenntnis nur, wenn nötig und so viel wie notwendig!“

- Jede OE hat in Abhängigkeit von ihrer Größe, Struktur, Aufgabenspektrum und Gefährdungssituation selbst individuelle Analysen durchzuführen und entsprechende Sicherheitsvorkehrungen zu treffen (verantwortlich: Leitung der OE).
- Basis jeder Analyse ist die Bestimmung von Inhalt und Umfang „schützenswerter Betriebsgeheimnisse“.

Geltungsbereich und Zuständigkeiten

- Der Geltungsbereich ist die EWN am Standort Lubmin/Rubenow einschließlich Zwischenlager Nord (ZLN) und der Betriebsteil Rheinsberg.
- Bei allen Zweifelsfragen, die sich aus dem Umgang mit Verschlusssachen oder Betriebsgeheimnissen ergeben, wenden Sie sich an das zentrale Sicherheitsorgan für Angelegenheiten des Geheimschutzes den/die

Sicherheitsbevollmächtigte/n (SiBe):

Thea Weidermann
Telefon +49 38354 4-8694
Telefon2 +4938354 4-4372
Mobil +49 174 6942537
thea.weidermann@ewn-gmbh.de

Stellvertreter:
Sebastian Rieck
Telefon +49 38354 4-8160

Mobil +49 175 3201690
sebastian.rieck@ewn-gmbh.de

DATENSCHUTZ

Schutz personenbezogener Daten

Datenschutz ist Ihr Grundrecht

In der EU

- Artikel 8 der EU-Grundrechtecharta: „Schutz personenbezogener Daten“

In Deutschland

- Artikel 1 und 2 des Grundgesetzes

Datenschutz

=

Schutz der Person

Informationssicherheit

=

Schutz der Informationen/Daten

Was ist das Ziel der DS-GVO?

- Die Europäische Datenschutz-Grundverordnung soll sicherstellen, dass **EU-Bürger datenschutzrechtlich geschützt** sind und gleichzeitig der **freie Datenverkehr innerhalb des EU-Binnenmarkts gewährleistet** wird.
- Verbraucher erhalten mehr Rechte.
- Für Unternehmen bedeutet das **strengere Auflagen und mehr Pflichten**.
- Alle Anforderungen haben eines gemeinsam: Unternehmen benötigen einen genauen **Überblick über** die von ihnen gespeicherten **Daten** und verwendeten **Verfahren**.
- Es gilt das **Marktortprinzip**: Die DS-GVO ist für internationale Unternehmen verbindlich, wenn sie ihre Dienste in EU-Staaten anbieten.

Was sind „personenbezogene Daten“?

Alle Angaben, die sich auf eine identifizierte oder identifizierbare Person beziehen, beispielsweise:

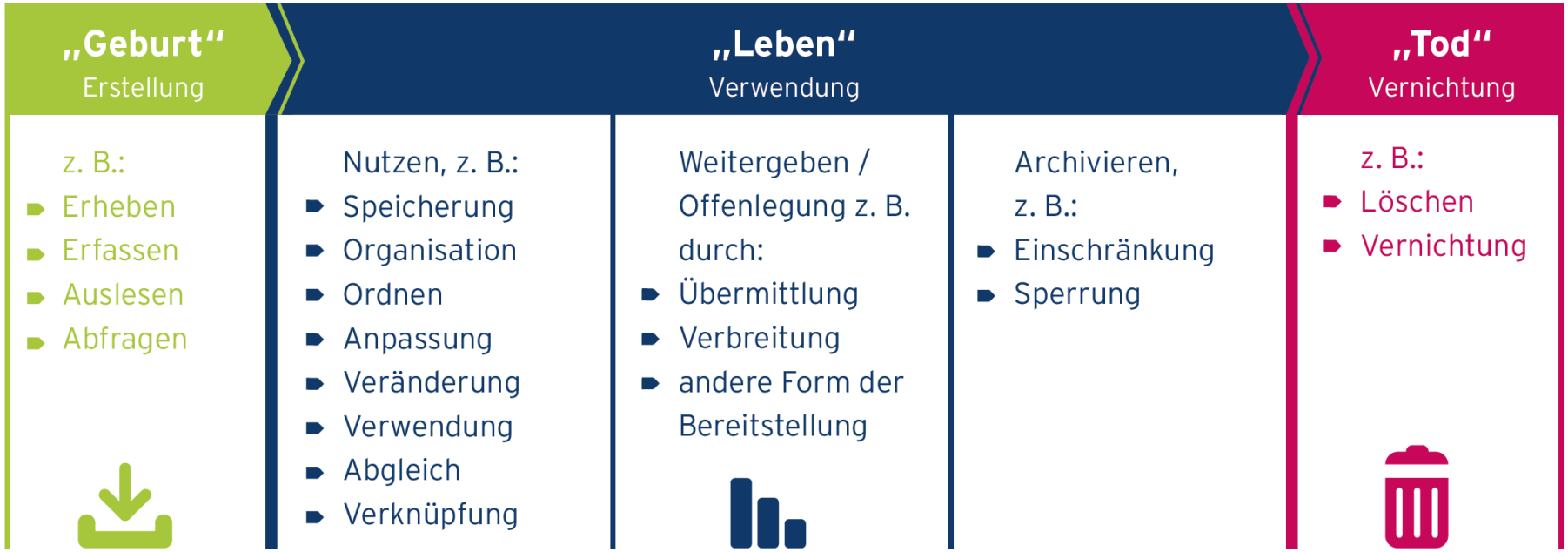
- Namen
- Adresse
- Geburtsdatum
- Telefonnummer
- Vermögen / Besitz
- Gehalt
- Fotos
- Personalnummer
- Benutzerkennung
- Arbeitsverhalten / Arbeitsergebnisse
- Maschinenbezogene Nutzungsdaten

Besonders sensible Daten sind besondere Kategorien personenbezogener Daten:

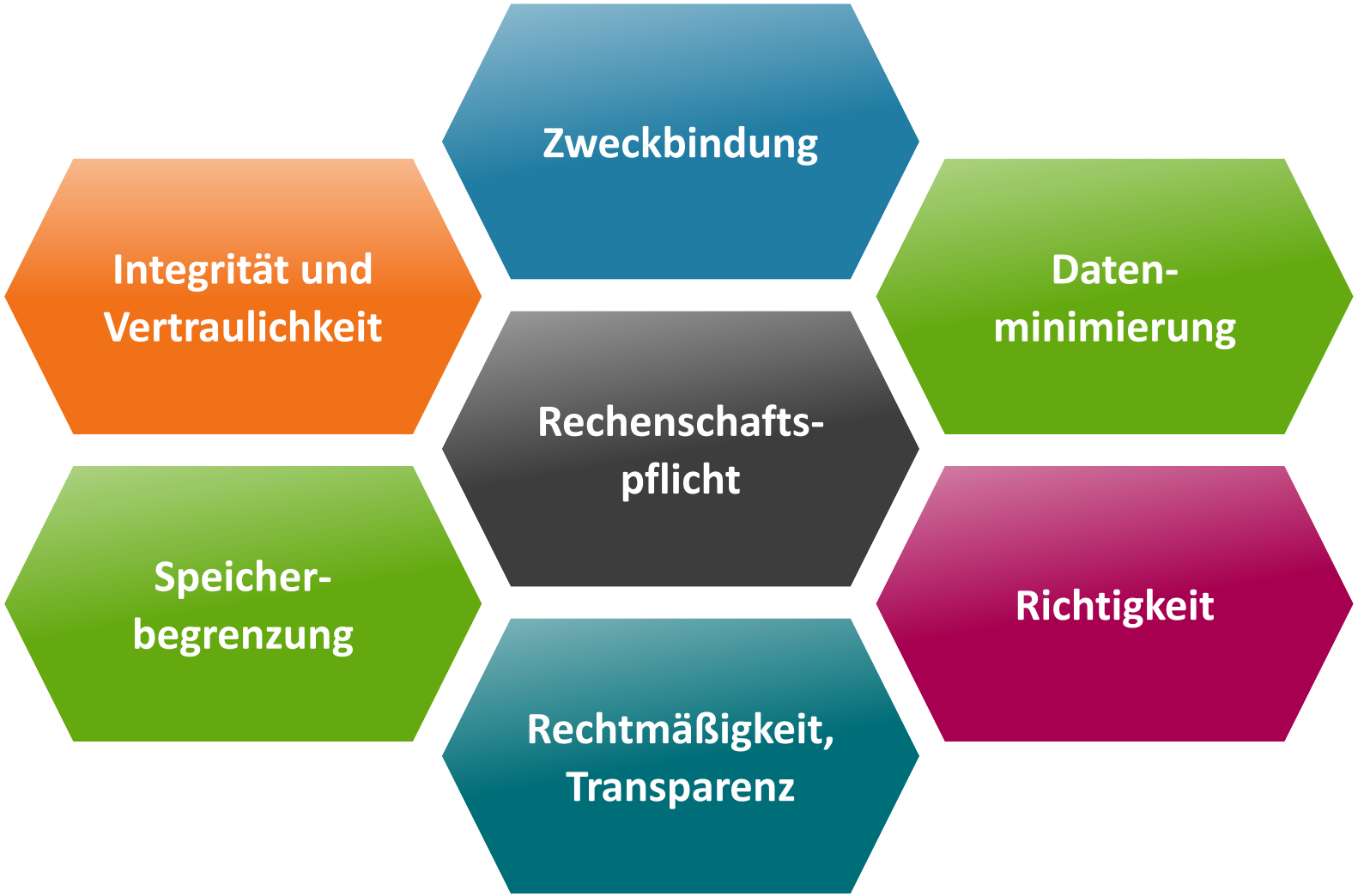
- Genetische und Gesundheitsdaten
- Biometrische Daten (bspw. Fingerabdrücke)
- Gewerkschaftszugehörigkeit
- Sexualleben / sexuelle Orientierung
- Rassistische Zuschreibungen oder ethnische Herkunft
- Politische, religiöse oder weltanschauliche Überzeugung

Was bedeutet „Verarbeitung“ personenbezogener Daten?

- Unter der Verarbeitung wird die Erstellung, Verwendung und Vernichtung der personenbezogenen Daten verstanden („Lebenslauf“ der Daten)
- Der Anwendungsbereich des Datenschutzes umfasst jede Verarbeitung von personenbezogenen Daten, sowohl in digitaler als auch in analoger Form.

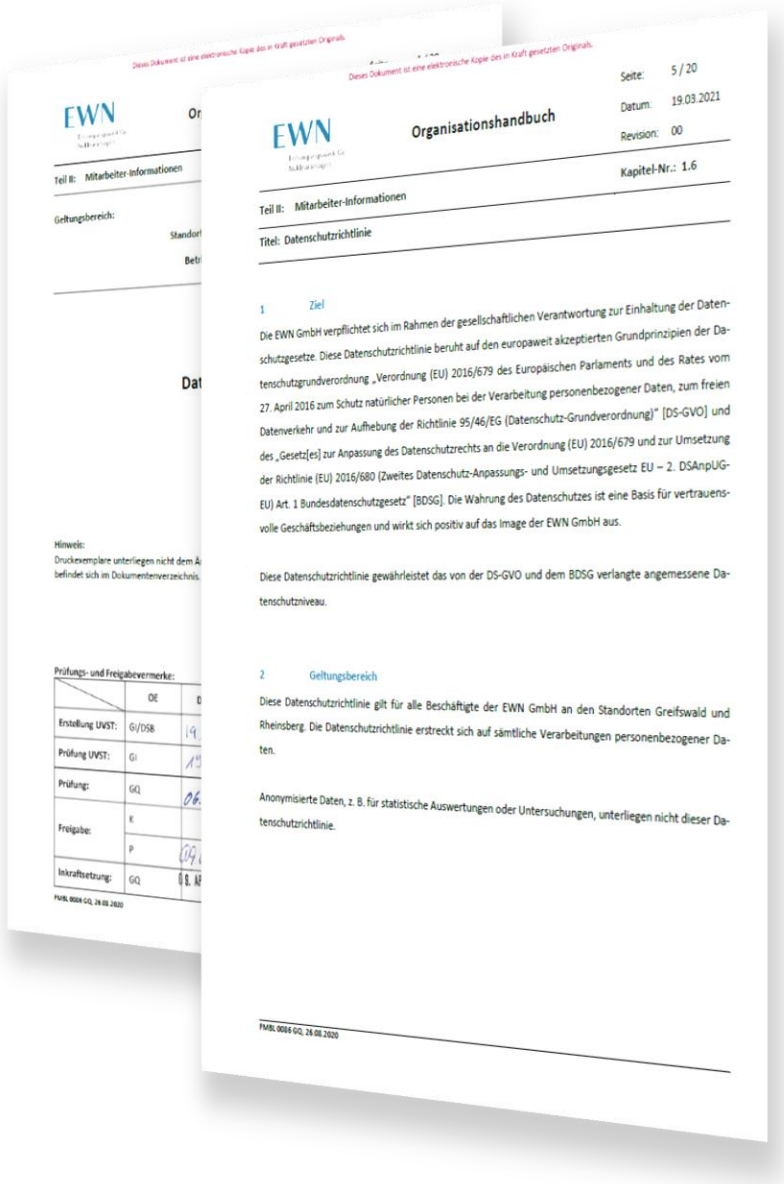


Bei der Verarbeitung sind „Grundsätze“ einzuhalten



Datenschutzrichtlinie der EWN

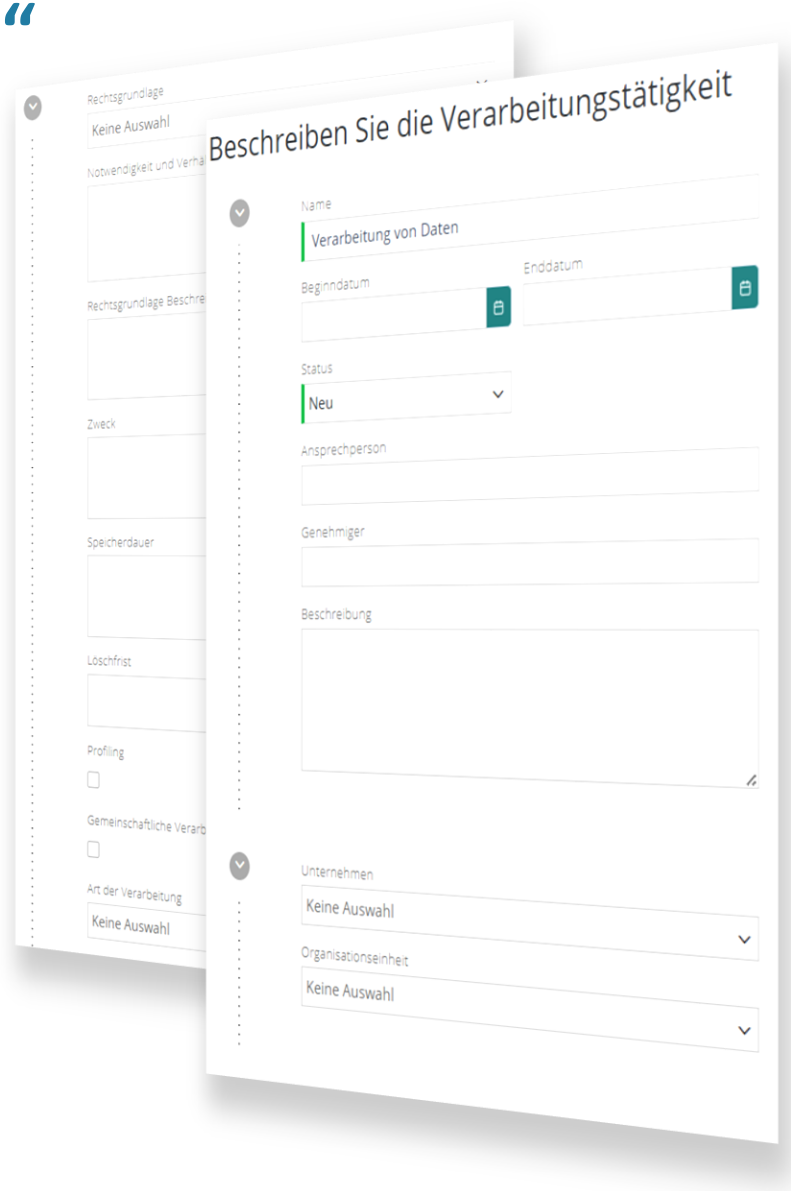
„Diese Datenschutzrichtlinie gilt für alle Beschäftigte der EWN GmbH an den Standorten Greifswald und Rheinsberg. Die Datenschutzrichtlinie erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten.“



1) Konventionelles Regelwerk F1.3 RL 02

Meldung von „Verarbeitungstätigkeiten“

- Verantwortliche müssen ein Verzeichnis aller Verarbeitungstätigkeiten führen.
- Als Verarbeitungstätigkeit sind dabei alle Verarbeitungen personenbezogener Daten, einschließlich Papierunterlagen, zu verstehen.
- Alle Verarbeitungstätigkeiten sind der Datenschutzbeauftragten mittels des dafür vorgesehenen Formulars zu melden.
- Die Meldung kann um projekt- / prozessinterne Dokumentation ergänzt werden, um Mehrarbeit zu vermeiden.



DSMS der EWN: https://rms.ewn.zz/crisomwebaccess_dsms/DSMS-EWN/

Mögliche Sanktionen gegenüber Beschäftigten

Aufgaben der Datenschutzbeauftragten

- Überwachung der Einhaltung des Datenschutzrechts.
- Unterrichtung und Beratung hinsichtlich der Pflichten aber auch der Rechte der Beschäftigten nach den geltenden Datenschutzvorschriften und
- Unterstützung bei der Bewertung von technischen und organisatorischen Maßnahmen
- Zur Geheimhaltung und Verschwiegenheit verpflichtet.
- Zusammenarbeit mit den Aufsichtsbehörden.

Kontaktdaten der Datenschutzbeauftragten

Zuständig für die Einhaltung des innerbetrieblichen Datenschutzes ist:

Angela Bialke
Datenschutzbeauftragte
Telefon +49 38354 4-5307

Hendrik Gralla
Stellv. Datenschutzbeauftragter
Telefon +49 38354 4-9313

datenschutz@ewn-gmbh.de
https://intranet.intern/
beauftragte/datenschutzbeauftragte

Zuständige Aufsichtsbehörde für die EWN GmbH als Bundesunternehmen:

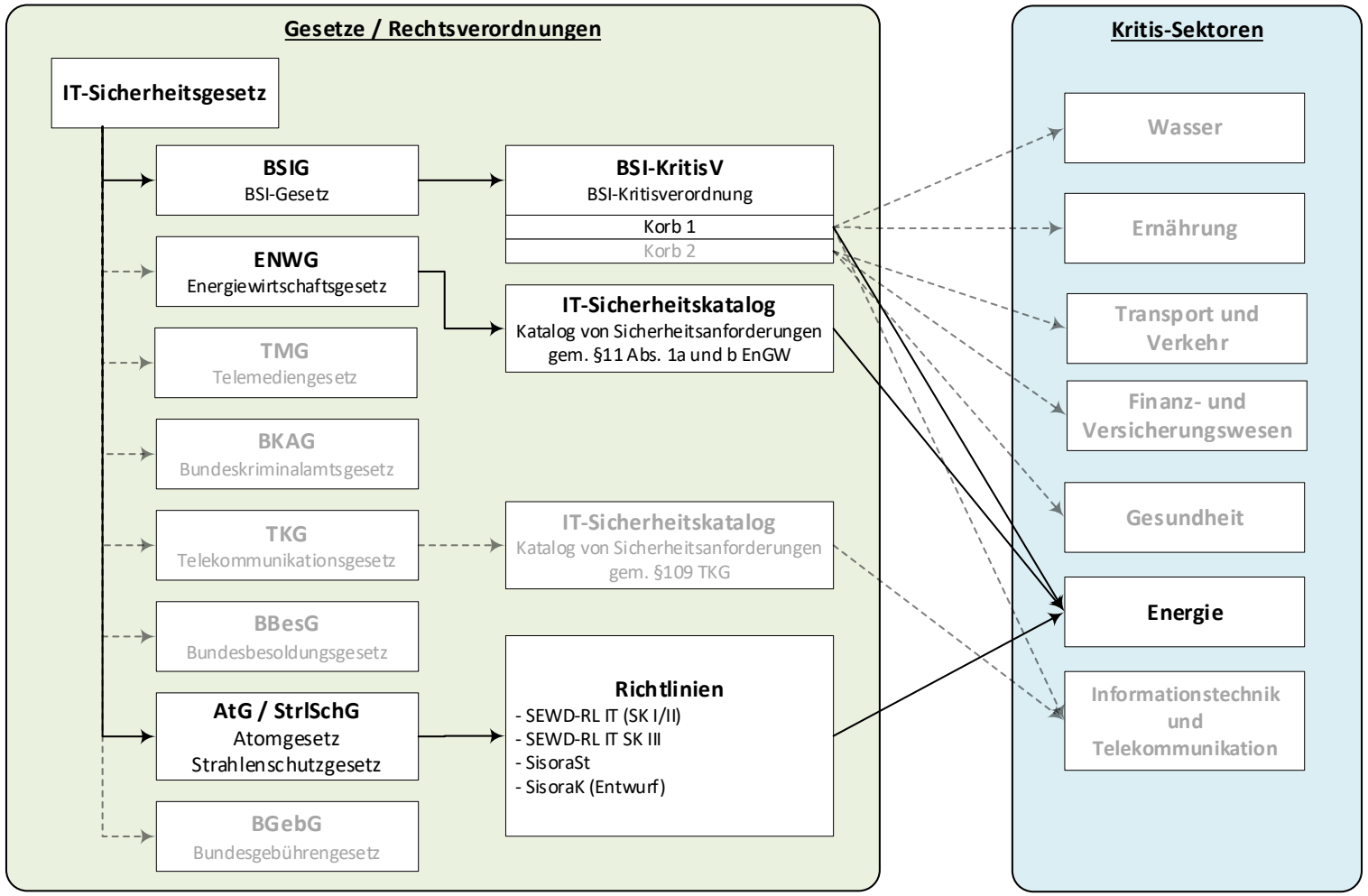
BfDI
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Datenschutzvorfälle werden in Abstimmung mit der Datenschutzbeauftragten an die Aufsichtsbehörde gemeldet.

IT-SICHERHEIT

Schutz von der elektronischen Datenverarbeitungssysteme (Hardware und Software)

Gesetze und Rechtsverordnungen für den Bereich der IT-Sicherheit



Internet und E-Mail

- Für alle Mitarbeitenden gilt die Gesamtbetriebsvereinbarung 01/2017[1)]:

  „Nutzung von Informations- und Kommunikationstechnologien“

  - Ein- und ausgehender dienstlicher E-Mail-Verkehr wird zur Wahrung gesetzlicher Aufbewahrungsfristen automatisch archiviert (10 Jahre)
  - Internet-Verbindungsdaten (Datum, Uhrzeit, Website, IP-Adresse, ggf. Datenmengen) werden protokolliert und für 7 Tage gespeichert.
    - Kontrollen durch Systemadministratoren im Zusammenwirken mit dem betrieblichen Datenschutzbeauftragen und dem Betriebsrat sind möglich.
  - Die private Nutzung der betrieblichen E-Mail-Adressen ist nicht gestattet.
  - Private Nutzung von eigenen E-Mail-Adressen bei externem Provider (über den Browser) und die Internetnutzung für private Zwecke ist nur kurzzeitig und gelegentlich gestattet.

1) https://intranet.intern/personal/betriebsvereinbarungen

Daten und Datenträger

- Für alle Mitarbeitenden gilt der IT-Management-Prozess [1)] :

  „Datenverarbeitung“

  - Unternehmenseigene Daten dürfen nicht auf privaten Computern bearbeitet oder gespeichert werden.
  - Private Daten dürfen nicht auf Unternehmenseigenen Computern bearbeitet oder gespeichert werden.
  - Private Technik ist nicht in der EWN einzusetzen
    - Ausnahmen sind schriftlich durch die zuständige Abteilungsleitung und die IT-Abteilung zu regeln
  - Datenträger (USB-Sticks…) sind einer Virenprüfung zu unterziehen.

1) Konventionelles Regelwerk U3 PZ 01

Zuständigkeit

- Bei Fragen oder Ereignissen, welche die IT-Sicherheit betreffen, wenden Sie sich bitte an die für den Standort Lubmin/Rubenow zuständigen

IT-Sicherheitsbeauftragten der EWN (ITSb):

Alexander Förster
Telefon +49 38354 4-5824
Mobil +49 1515 1613799

it-sicherheit@ewn-gmbh.de

Stellvertreter:
Hendrik Gralla
Telefon +49 38354 4-9313

COMPLIANCE

Einhaltung von Vorgaben und Standards

Compliance

- Verpflichtung zur Einhaltung von
  - gesetzlichen Bestimmungen und
  - regulatorischen Standards.
- Erfüllung selbst gesetzter, ethischer Vorgaben und Anforderungen.
- Korrektes Verhalten in allen Geschäftsprozessen.
- Es gilt der Compliance-Kodex[1)] der EWN-Gruppe.
- Die Unterweisung zum Thema Compliance ist regelmäßig durch die Führungskräfte zu veranlassen.

1) https://intranet.intern/compliance

Beauftragte für Compliance

Zuständigkeitsbereich: EWN-Gruppe, EWN GmbH und ZLN GmbH:

Ingo Schulz

Telefon +49 38354 4-8190
Mobil +49 151 18447984

ingo.schulz@ewn-gmbh.de

ZUSAMMENFASSUNG
für die tägliche Praxis

Informationen schützen im Alltag

- Beachten Sie die Regelwerke der EWN.
- Es dürfen nur die Daten erhoben und verarbeitet werden, die zur Aufgabenerfüllung notwendig sind.
- Geben Sie unbefugt keine Informationen an Dritte (Polizei, Sozialamt, Krankenkasse, Unbekannte etc.) weiter. Bestehen Sie auf eine schriftliche Anfrage und die Nennung der Rechtsgrundlage!
- Verwehren Sie Unbefugten die Einsicht in Unterlagen! Das gilt für unbefugte Mitarbeitende und Externe gleichermaßen.
- Über dienstliche und personenbezogene Informationen ist – insbesondere außerhalb des Arbeitsverhältnisses – Vertraulichkeit zu wahren.

Informationen schützen im Alltag – Arbeitsplatz

- Clean-Desk-Prinzip: Halten Sie Ihren Arbeitsplatz aufgeräumt.
- Sperren Sie immer Ihren Arbeitsplatzrechner (Win + L), auch wenn Sie Ihr Büro nur kurz verlassen. Schließen Sie Ihren Raum ab, wenn Sie das Büro für längere Zeit verlassen (bspw. für Termine, Pausen).
- Verwahren Sie Daten, Datenträger und Ausdrucke stets sicher, bspw. in verschlossenen Schränken – insbesondere bei der mobilen Arbeit.
- Verwenden Sie sichere Passwörter und vermeiden Sie Mehrfachverwendung.
- Geben Sie persönliche Passwörter oder Benutzerkennungen niemals weiter.
- Nutzen Sie zum Verwalten Ihrer persönlichen, dienstlichen Passwörter den Passwortmanager „KeePass“
  - auf neuer Hardware vorinstalliert
  - alternativ über Softwareantrag im Self-Service-Portal zu bestellen

Informationen schützen im Alltag - Datenübermittlung

- E-Mails und Telefaxe sind nicht sicherer als Postkarten! Versenden Sie vertrauliche Daten daher NICHT per Fax oder als unverschlüsselte E-Mail.
- Nutzen die gängigen Verschlüsselungsmöglichkeiten[1)] in der EWN:
  - Cryptshare (E-Mail)
  - VeraCrypt (längerfristige Verschlüsselung besonders sensibler Daten)
  - 7-Zip (einmalige Verschlüsselung von Dateien)
  - **Nicht geeignet** ist der Kennwortschutz von MS-Office.
- Kontrollieren Sie bei E-Mails die Empfängerliste, insbesondere bei der Nutzung der „Allen-Antworten-Funktion“.
- Versenden oder transportieren Sie Unterlagen nur in verschlossenen Umschlägen oder Behältern.

1) Achtung: verschlüsselte Daten können NICHT wiederhergestellt werden, wenn das Passwort verloren geht oder die Datei beschädigt wird.

Informationen schützen im Alltag – Daten & Datenträger

- Entsorgen Sie dienstliche Dokumente in den dafür vorgesehenen Sammelbehältern oder schreddern Sie diese mit geeigneten Aktenvernichtern.
- Datenträger (USB-Sticks, Festplatten etc.) über KDI entsorgen.
- Leeren Sie nach dem Löschen von Dateien auch den Windows-Papierkorb.
- Melden Sie den unbeabsichtigten Verlust oder eine unautorisierte Freigabe von Daten **unverzüglich** Ihrem Vorgesetzten und / oder dem zuständigen Beauftragten, z. B. wenn Sie Dokumente oder mobile Geräte oder Speicher wie USB-Sticks verlieren!
- Machen Sie sich mit den spezifischen Regelungen zu Datenschutz und IT-Sicherheit im Unternehmen und in ihrem Fachbereich vertraut!

Datenschutz im Alltag

- Beschäftigte dürfen personenbezogene Daten, welche ihnen im Rahmen ihrer Tätigkeit zu Kenntnis kommen, nicht für private oder eigene wirtschaftliche Zwecke nutzen, an Unbefugte weitergeben oder diesen zugänglich machen.
- Achten Sie besonders auf die Wahrung der Vertraulichkeit beim Einsatz mobiler Geräte wie Smartphones, Notebooks oder Tablets! Dies gilt bspw. auf Bahnfahrten: lassen Sie die Geräte niemals unbeaufsichtigt. Lassen Sie keine Mitreisenden auf den Bildschirm blicken.
- Besondere Sorgfalt gilt auch für die Nutzung privater Informationen von Mitarbeitern: fragen Sie Ihre Kollegen um Erlaubnis, BEVOR Sie private Telefonnummern, E-Mail-Adressen oder Messenger-IDs an andere Kollegen weitergeben oder für Gruppenaktivitäten verwenden.

Besprochene betriebsinterne Regelwerke

- *IT-Management-Prozess „Datenverarbeitung“*
  (Konventionelles Regelwerk U3 PZ 01)
- *Informationssicherheits-Richtlinie „Umgang mit Verschlusssachen“*
  (Konventionelles Regelwerk F1.2 RL 01)
- *Informationssicherheits-Richtlinie „Datenschutz“*
  (Konventionelles Regelwerk F1.3 RL 02)
- *Compliance-Kodex*
  (https://intranet.intern/compliance)

Wir setzen Maßstäbe.
Mit Sicherheit.

Herzlich willkommen und viel Erfolg!

Angela Bialke
Telefon +49 38354 4 - 5307 | angela.bialke@ewn-gmbh.de | www.ewn-gmbh.de